Secret sharing without monitoring signal disturbance

Kejin Wei[1,*], Xiuqing Yang[2], Haiqiang Ma[3,†], Changhua Zhu[4],

[1] *Guangxi Key Laboratory for Relativistic Astrophysics, School of Physics Science and Technology, Guangxi University, Nanning 530004, China*

[2] *School of Science, Beijing Jiaotong University, Beijing 100044, China*

[3] *School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[4] *State Key Laboratory of Integrated Services Networks, Xidian University, Xian, Shanxi 710071, China*

[*] *kjwei@gxu.edu.cn*

[†] *hqma@bupt.edu.cn*

(Dated: January 3, 2017)

Abstract

Secret sharing, in which a dealer wants to split a secret in such a way that any unauthorized subset of parties is unable to reconstruct it, plays a key role in cryptography. The security of quantum protocols for the task is guaranteed by the fact that Eve's any strategies to obtain secret information from encoded quantum states should cause a disturbance in the signal. Here, we propose a quantum secret sharing (classical information) scheme for N parties based on totally different principle in which monitoring signal disturbance is no longer need. In this scheme, the secret is divided among several partners by sequential transmissions of a L-dimensional qudit state, which can be practically implemented using a conventional laser and some standard off-the-shelf components. Our scheme paves a novel and practical way for quantum secret sharing.

I. INTRODUCTION

Secret sharing is a common task in cryptography and information processing. Its objective being to split a secret in such a way that any unauthorized subset of parties is unable to reconstruct it. For example, suppose that the manager of a bank wants to share a secret code of a safe to three vice managers who are not wholly trusted. He may desirably split and distribute the secret code in way that a vice manager alone is incapable to open the safe, but at least two vice managers are required. In 1979, Blakely [1] and Shamir [2] independently proposed the first secret sharing scheme in which mathematical algorithms are used to split the secret and sub-secrets are distributed by classical communication. However, like other classical cryptography, classical secret sharing schemes are threatened with the rising of computation rate, particularly with the development of quantum computation, and are vulnerable to intercept-resend attacks. Solutions for these problems are introducing quantum resources, which can lead to information-theoretically secure communication [3–5]. Based on three-particle Greenberger-Horne-Zeilinger (GHZ) entangled states, Hillery *et al.* [6] proposed a pioneering scheme for three-parties (classical) secret sharing and its variations are widely studied in the context of quantum secret sharing (QSS)[7–10] (it differs from quantum state sharing, where a quantum state rather than a classcial message is shared [11, 12]). Due to the difficulty of generating required multi-party entangled states for the growing number participants, entanglement-based protocols are not easily implemented and are not scalable so that a few experimental demonstrations for entanglement-based protocols have been reported in recent years [13–15].

In contrast, QSS protocols without entanglement are more scalable and have a rapid development both in therotical and experimental aspects [16–33] . Nonetheless, developing a secure and efficient entanglement-free QSS (EF-QSS) protocol is still a research challenge in the field since some previous EF-QSS protocols are impractical with current technology and the security of exsiting EF-QSS protocols are not as roubust as that of quantum key distribution (QKD). For example, the first EF-QSS protocol was proposed by Zhang *et al.* [27], however, the protocol required quantum memories compromising its practical application with current technology. Futhermore, it was latter proven that the scheme is unable to reach the security level as it claimed [28, 29]. For another example, with the same motivation, Schmid *et al.* [30] presented a protocol only requiring sequential communication of

a single qubit from partner to partner. Alought its practicality and scalability have been experimentally proven over telecommunication fiber [17, 23–25], it was also shown to be also susceptible to the participant attack [31–33].

A long-held belief for QSS, the same as other issues in quantum cryptography, is that the security of QSS is based on Heisenberg's uncertainty principle, which dictates that Eve's any strategies to obtain secret information from encoded quantum states should cause a disturbance in the signal. Recently, in the context of QKD, Sasaki *et al*. published a novel protocol, named "round-robin differential phase shift (RRDPS)" [34], which relies on an entirely different principle and is no need to monitor the signal disturbance. Subsequently, Demonstrations of RRDPS and its variation version have been independently reported [35–37]. This new protocol gives a new way to connect the nature of quantum mechanics to secure communication. With the success of RRDPS, it was then quite natural to ask if this different principle can be used in QSS.

Here, based on the RRDPS protocol, we propose a novel QSS scheme for N parties without monitoring signal disturbance, making the scheme entirely different from previous QSS protocols. In our scheme, the secret is divided among several partners by sequential transmissions of a L-dimensional qudit state, which can be practically implemented using a conventional laser and some standard off-the-shelf components. Moreover, as our scheme is entanglement-free scheme which only requires a qudit state; it has obvious advantages in scalability comparing to entanglement-based QSS protocols. We also present a practical implementation for the proposed scheme with standard off-the-shelf components, implying that our scheme is realizable and practical with current technologies.

II. SECRET SHARING WITH A SINGLE QUDIT

The schematic of our quantum secret sharing scheme is shown in Fig. 1. The scheme runs as follows.

(i) The dealer R_1, who by the nature of secret sharing is always supposed to be a trusted party, prepares an L-dimensional qudit state as

$$|\psi_1\rangle = \frac{1}{\sqrt{L}} \sum_{k=1}^{L} |k\rangle, \tag{1}$$

where $|k\rangle$ denotes L-dimensional orthonormal base vector and the state in which the photon

is in the kth pulse.

(ii) For $n = 2, 3...N$, the party R_n encodes a random $L-$bit string $s_{n1}s_{n2}...s_{nL} \in \{0,1\}^{\otimes L}$ to the qudit $|\psi_{n-1}\rangle$ received from R_{n-1} by applying an unitary transformation

$$Z_L^n = \sum_{k=1}^{L} (-1)^{s_{nk}} |k\rangle \langle k| . \tag{2}$$

Simply connect Eqs. (1) and (2), one gets

$$\begin{aligned} Z_L^n |\psi_1\rangle &= (\sum_{k=1}^{L} (-1)^{s_{nk}} |k\rangle \langle k|)(\frac{1}{\sqrt{L}} \sum_{k=1}^{L} |k\rangle) \\ &= \frac{1}{\sqrt{L}} \sum_{k=1}^{L} (-1)^{s_{nk}} |k\rangle. \end{aligned} \tag{3}$$

R_n's operation transforms $|\psi_{n-1}\rangle$ into $|\psi_n\rangle$ as

$$\begin{aligned} |\psi_n\rangle &= Z_L^n |\psi_{n-1}\rangle \\ &= (\frac{1}{\sqrt{L}} \sum_{k=1}^{L} (-1)^{(s_{2k}+...+s_{nk})} |k\rangle), \end{aligned} \tag{4}$$

which is then sent to subsequent party R_{n+1} except the case in party R_N who sends the qudit back to the dealer R_1. Therefore, after having passed all parties ($n = 1, 2...N$), the original qudit will be back to R_1 in the state

$$|\psi_N\rangle = (\frac{1}{\sqrt{L}} \sum_{k=1}^{L} (-1)^{(s_{2k}+...+s_{Nk})} |k\rangle). \tag{5}$$

(iii) Once receiving the state $|\psi_N\rangle$, R_1 generates an independent random number $r \in \{1, ..., L\}$ and measure the value $s_i \oplus s_j$ through an optical interference measurement M, where $s_i = (s_{2i} + ... + s_{Ni}) \bmod 2$, $s_j = (s_{2j} + ... + s_{Nj}) \bmod 2$ with indices $\{i, j\} \subset \{1, ..., L\}$ satisfying $i - j = \pm r (\text{mod } L)$ and the symbol $\oplus$ represents summation modulo 2. For this purpose, in the interference measurement M, R_1 splits each input to two paths of a variable interferometer and tries to observe a phase difference between $|i\rangle$ and $|j\rangle$ by adjusting a random delay r of one of the path and observing detectors' outcomes. Whenever the phase difference between $|i\rangle$ and $|j\rangle$ is observed, R_1 broadcasts $\{i, j\}$ to other parties in an authenticated public channel but keeps the observed phase difference as his sifted key bit S_1. Subsequently, with the stated indices $\{i, j\}$, the party R_n ($n = 2..., N$) records $S_n = s_{ni} \oplus s_{nj}$ as his sifted bit. At this time every party holds a private secret key bit

S_n and these key bits exhibit perfect correlations such that any subset of $N-1$ parties is able to infer the secret key bit of the remaining party, if and only if all the $N-1$ parties collaborate and share among themselves their private secret key bit S_n. While if a subset of less than $N-1$ parties attempt to sidestep the others, no one can obtain any information. For example, if $R_2 ..., R_N$ want to know the secret key bit of the last party R_1, they just share their secret key bit S_n with each other and then compute $S_1 = S_2 \oplus ... \oplus S_N$. By repeating steps (i) to (iii) all parties can accumulate sufficient key bit sequences that suffices for the task of secret sharing. It is worth mentioning here that the equations $S_1 = S_i \oplus S_j = [(s_{2i} + ... + s_{Ni}) \ mod \ 2] \oplus [(s_{2j} + ... + s_{Nj}) \ mod \ 2]$ and $S_1 = S_2 \oplus ... \oplus S_N = (s_{2i} \oplus s_{2j}) \oplus ... \oplus (s_{Ni} \oplus s_{Nj})$ are equal. A simple proof can be given as follow. In the former equation, when $S_1 = 0$, it is implying that S_i and$S_j$have the same parity, i.e. the number of items with a bit value of 1 in S_i andS_j is even or odd. So, using the latter equation, in which Boolean operations operate bit-by-bit, the final result is always equal to 0. For the case of $S_1 = 0$, with a similar analysis, the result of the latter equation is always equal to 1.

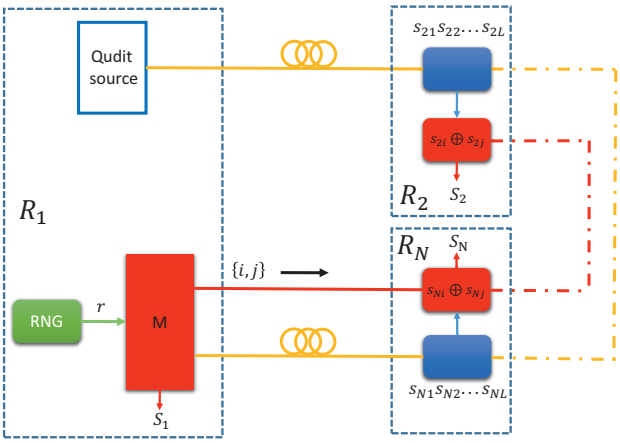

FIG. 1. (Color online) Conceptional schematic of proposed QSS protocol. A qudit is prepared by a Qudit source in the party R_1, then it is subsequently sent to $N-1$ parties. Each party from $n = 2, ..., N$ modulates the qudit with a private L-bit string $s_{n1}s_{n2}...s_{nL}$ and the last party R_N sends it back to R_1, who then performs an optical interference measurement M with an input r from a random number generator (RNG). Whenever a photon is observed from the superposed $|i\rangle$ and $|j\rangle$, R_1 public $\{i,j\}$ and records the measurement result as his sifted key bit S_1. The other parties compute $S_n = s_{ni} \oplus s_{nj}$ as their sifted bit with the indices $\{i,j\}$.

III. SECURITY ANALYSIS

In comparison to QKD, analysing the security of QSS protocols is a more complex process because of involving multiple participants who are uncertainly honest or dishonest. Furthermore, a dishonest participant, who legally knows partial information and can lie to avoid to be detected, is more dangerous than an outside eavesdropper [38, 39]. In this way, the main goal for the security of our QSS scheme mainly concerns the prevention of participant attacks which are launched by a dishonest participant or a group of cheating participants. What we remark that since the cheating participants complicate the security analysis of QSS protocols, as far as we know, most of previous protocols have yet not been proven to be unconditionally secure against arbitrary participant attacks and just can be deal with particular attacks. In our analysis, we will also analyse the robustness of our scheme against some particular attacks. Furthermore, we treat the dealer R_1 as a trusted party with trusted devices, which is a reasonable assumption in QSS.

Consider that a dishonest participant, say R_n^*, to eavesdrop the key of the previous participant R_{n-1}, performs general attacks to the qudit state $|\psi_{n-1}\rangle$ which he received from R_{n-1}. For example, he can entangle the qudit to an ancilla and possibly get part of the infromation in the ancilla. Then he uses this collected infromation to retrieve the key of R_{n-1}. However, such general attacks are unavilable to our scheme since, note that, what R_n^*'s intervention can obtain is the decision of index i, however, the final key bits are decided with the combination of the index i and index j, which is randomly generated by the trusted party R_1. Hence, R_n^* can not gain any key bits of R_{n-1} from the intervention of the transmitted qudit state $|\psi_{n-1}\rangle$. Consider anther analysis procedure as follow. For any general attacks to $|\psi_{n-1}\rangle$, we can regard the parties $R_1, ..., R_{n-1}$ as a single party, and the remaining parties R_n and R_1 act as a measuring party with some additional encodings. Thus, the attacks can be viewed as an eavesdropper in RRDPS protocol, which has been proven to be unconditionally secure [34]. Although it has been proven that RRDPS is insecure with untrusted measurement device [40], our scheme is immune to such attacks because the measurement device is in the dealer R_1 who is naturally supposed to a trusted party with trusted devices. This case can extend to more general case, in which a group of cheating participants use some general attacks to collected information from their received qudits, then they share this collected information with each other to retrieve the key of the

remaining parties. Still, they ought not to be successful because the information from the qudits is not effective to reveal the key bits of the remaining parties.

What is impressive here is that the above security proof is not related with how much signal disturbance has been caused by Eve, making our protocol is entirely different from previous QSS protocols in which the basic physics behind the security are Heisenberg's uncertainty principle.

IV. PRACTICAL IMPLEMENTATION OF PROPOSED QSS PROTOCOL

Our scheme can be implemented by simply modifying the setup of RRDPS protocol, which contains a weak coherent laser and a Mach-Zehnder interferometer (MZI). As shown in Fig. 2, To prepare the qudit $|\psi_1\rangle$, Alice's laser emits a train of L pulses with time interval T. After being attenuated by a variable attenuator (ATT) to a single-photon level, the train is sent to the next party R_2 and is sequentially communicated from R_2 to R_N. For the party R_n $(n = 2, 3...N)$, he modulates the train received from previous party R_{n-1} by a phase modulator (PM_n) with a phase shift $\{0, \pi\}$ according to an $L-$bit string $s_{n1}s_{n2}...s_{nL}$ $\in \{0,1\}^{\otimes L}$, and then sends it to the subsequent party R_n except that in the case of the last party R_N who sends the train back to R_1. Once receiving the train again, R_1 splits the train to two paths of a variable MZI and performs a single-photon interference with randomly adjusting a delay $r * T$ of one of the path. The delay $r * T$ is controlled by a variable delay line with an input $r \in \{1, ..., L-1\}$ from a random number generator (RNG). After observing a detection in two single-photon detectors (SPD_1, SPD_1), R_1 records the phase difference as his sift bit S_N and announces the corresponding indices $\{i, j\}$. The other parties compute $S_n = s_{ni} \oplus s_{nj}$ as their sifted bit .

V. CONCLUSION

In summary, we propose a novel QSS scheme for N parties. Unlike other quantum schemes, our scheme is based on an entirely different principle, in which monitoring the signal disturbance is no longer need. Comparing to entanglement-based QSS protocols, our scheme has obvious advantages in practicality and scalability because the secret is divided among several partners by sequential transmissions of an $L-$dimensional qudit state, which

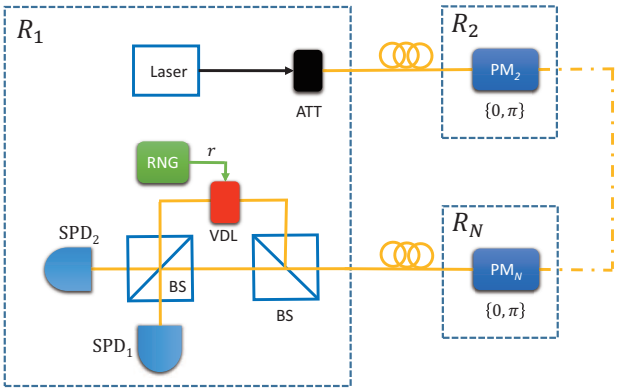

FIG. 2. (Color online) Schematic of a practical implementation for proposed QSS scheme. PM_1, PM_2, PM_N, phase modulator; BS, beam splitter; VDL, variable delay line; RNG, random number generator; SPD_1, SPD_2, single-photon detector.

can be implemented using a conventional laser and some standard off-the-shelf components. we discuss the security of our scheme and also present a practical implementation for the proposed scheme, implying that our scheme is feasible and practical with current technologies.

VI. ACKNOWLEDGEMENTS

This work was supported by the Guangxi Science Foundation (Grant No. 2014GXNSFBA118004, 2013GXNSFFA019001); the Fund of State Key Laboratory of Information Photonics and Optical Communications (Beijing University of Posts and Telecommunications) No. IPOC2016ZT09, the National Natural Science Foundation of China Grant No. 61178010 and No. 11374042; the Fundamental Research Funds for the Central Universities No. bupt2014TS01.

[1] G. R. Blakley, Proc. of the National Computer Conference, 1979 **48**, 313 (1979).

[2] A. Shamir, Commun. Acm **22**, 612 (1979).

[3] C. H. Bennett, G. Brassard, *et al.*, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175 (New York, 1984).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[5] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014).

[6] M. Hillery, V. Buek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[7] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[8] L. Xiao, G. Lu Long, F.-G. Deng, and J.-W. Pan, Phys. Rev. A **69**, 052307 (2004).

[9] M. H. Dehkordi and E. Fattahi, Quantum Inf. Process. **12**, 1299 (2013).

[10] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Phys. Rev. Lett. **114**, 090501 (2015).

[11] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[12] H. Lu, Z. Zhang, L.-K. Chen, Z.-D. Li, C. Liu, L. Li, N.-L. Liu, X. Ma, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett. **117**, 030501 (2016).

[13] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).

[14] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **95**, 200502 (2005).

[15] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007).

[16] I. C. Yu, F.-L. Lin, and C.-Y. Huang, Phys. Rev. A **78**, 012344 (2008).

[17] P. Scherpelz, R. Resch, D. Berryrieser, and T. W. Lynn, Phys. Rev. A **84**, 032303 (2011).

[18] X.-B. Chen, X.-X. Niu, X.-J. Zhou, and Y.-X. Yang, Quantum Inf. Process. **12**, 365 (2013).

[19] V. Karimipour and M. Asoudeh, Phys. Rev. A **92**, 030301 (2015).

[20] A. Tavakoli, I. Herbauts, M. Żukowski, and M. Bourennane, Phys. Rev. A **92**, 030302 (2015).

[21] H. Liu, H. Ma, K. Wei, X. Yang, W. Qu, T. Dou, Y. Chen, R. Li, and W. Zhu, Phys. Lett. A **380**, 2349 (2016).

[22] H. Qin and Y. Dai, Quantum Inf. Process. **15**, 2091 (2016).

[23] J. Bogdanski, N. Rafiei, and M. Bourennane, Phys. Rev. A **78** (2008).

[24] J. Bogdanski, J. Ahrens, and M. Bourennane, Opt. Express **17**, 1055 (2009).

[25] H.-Q. Ma, K.-J. Wei, and J.-H. Yang, Opt. Lett. **38**, 4494 (2013).

[26] K. J. Wei, H. Q. Ma, and J. H. Yang, Opt. Express **21**, 16663 (2013).

[27] Z.-J. Zhang, Y. Li, and Z.-X. Man, Phys. Rev. A **71**, 044301 (2005).

[28] F.-G. Deng, X.-H. Li, H.-Y. Zhou, and Z.-j. Zhang, Phys. Rev. A **72**, 044302 (2005).

[29] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, Phys. Lett. A **357**, 101 (2006).

[30] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **95** (2005).

[31] G. P. He, Phys. Rev. Lett. **98**, 028901 (2007).

[32] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **98**, 028902 (2007).

[33] He, G. Ping, Wang, and D. Z., Quantum Inf. Comput. **10**, 28 (2010).

[34] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475 (2014).

[35] J. Y. Guan, Z. Cao, Y. Liu, G. L. Shen-Tu, J. S. Pelc, M. M. Fejer, C. Z. Peng, X. Ma, Q. Zhang, and J. W. Pan, Phys. Rev. Lett. **114**, 180502 (2015).

[36] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nat. Photon. **9**, 832 (2015).

[37] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nat. Photon. **9**, 827 (2015).

[38] F.-G. Deng, X.-H. Li, H.-Y. Zhou, and Z.-j. Zhang, Phys. Rev. A **72**, 044302 (2005).

[39] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, Phys. Lett. A **357**, 101 (2006).

[40] Z. Cao, Z.-Q. Yin, and Z.-F. Han, Phys. Rev. A **93** (2016).